UNIFORM SAFEGUARDS FOR PROTECTION OF "CRITICAL SYSTEMS" PROCESSING INTELLIGENCE INFORMATION

Supplement
to
Security Policy
on Intelligence Information
in Automated Systems
and Networks
DCID 1/16, 4 January 1983

December 1984

* * * * * * * *

FOREWORD

The Deputy Director of Central Intelligence (DDCI) directed that security SAFEGUARDS be developed to reduce the vulnerabilities associated with processing information derived from sensitive intelligence sources and methods in "critical" automated systems and networks. These "critical systems" were identified by the senior members of the Intelligence Community and uniform assessments of the security of these systems were made using an early draft of these SAFEGUARDS. These SAFEGUARDS identify security requirements which, when satisfied, will significantly reduce the vulnerabilities identified in the assessments of the "critical systems." These SAFEGUARDS requirements are intended as a transitional step for the Intelligence Community to reduce security risks that are inherent in existing "critical systems." The Intelligence Community will use the trusted security products and services of the Department of Defense (DoD) Computer Security Center as soon as such products and services are developed and are available to be incorporated into the Community's inventory of automated systems. These SAFEGUARDS reflect the Director of Central Intelligence's (DCI) requirements for reducing near-term risks until trusted systems are available and therefore are intended to complement the DoD Computer Security Evaluation Criteria. The SAFEGUARDS are mandatory for all "critical systems" and voluntary for all other systems processing information derived from sensitive intelligence sources and methods. (U)

Table of Contents

Next 36 Page(s) In Document Denied

IX. GLOSSARY

ACCESS. A specific type of interaction between a subject and an object that results in the flow of information from one to the other. (U)

AUTHENTICATION. A positive identification, with a degree of certainty sufficient for permitting certain rights or privileges to the person or thing positively identified. (U)

COMPARTMENTED MODE. See Section VI. (U)

"CRITICAL SYSTEM." For this document, a "critical system" is a computer system processing and/or storing intelligence information that has been selected by senior officials in the National Security Community. (U)

DATAGRAM. A datagram is an internet protocol packet; the packet is made up of a header and trailer. For the purpose of this document the datagram is the equivalent packet of data as defined by the network being utilized. (U)

DCI. Director of Central Intelligence. (U)

DCID. Director of Central Intelligence Directive. (U)

DDCI. Deputy Director of Central Intelligence. (U)

DEDICATED MODE. See Section IV. (U)

ESCORT. Duly designated personnel who have appropriate clearances and access approvals for the material contained in the ADP system and are sufficiently knowledgeable to understand the security implications and to control the activities and access of the individual being escorted. (U)

ISSO. Information System Security Officer. (U)

INTELLIGENCE INFORMATION. For purposes of this policy statement, intelligence information means foreign intelligence, and foreign counterintelligence involving sensitive intelligence sources and methods, that has been classified pursuant to Executive Order 12356 (or successor order). "Foreign intelligence" and "counterintelligence" have meanings assigned them in Executive Order 12333. "Intelligence," as used herein, also includes Sensitive Compartmented Information (SCI) as defined in the DCI Security Policy Manual for SCI Control Systems, effective 28 June 1982. (U)

LOW WATER MARK. Of two or more security levels, the least of the hierarchical classifications, and the set intersection of the nonhierarchical categories. (U)

MULTILEVEL MODE. See Section VII. (U)

NFIB. National Foreign Intelligence Board. (U)

NSO. Network Security Officer. (U)

OBJECT. A passive entity that contains or receives information. Access to an object potentially implies access to information it contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bytes, words, fields, processors, video displays, keyboards, clocks, printers' network nodes, etc. (U)

SBI. Special Background Investigation. (U)

SENSITIVE COMPARTMENTED INFORMATION (SCI). All information and materials requiring special Community controls indicating restricted handling within present and future Community intelligence collection programs and their end products. These special Community controls are formal systems of restricted access established to protect the sensitive aspects of intelligence sources and methods and analytical procedures of foreign intelligence programs. The term does not include Restricted Data as defined in Section II, Public Law 585, Atomic Energy Act of 1954, as amended. (U)

SENSITIVITY LABEL. A piece of information that represents the security level of an object and that describes the sensitivity (e.g., classification) of the data in the object. (U)

SESSION. An activity for a period of time; the activity is access to a computer/network resource by a user; a period of time is bounded by session initiation (a form of logon) and session termination (a form of logoff). (U)

SESSION SECURITY LEVEL. The security level of a session is the low water mark of the security levels of: the user, the terminal, a level specified by the user, and the system from which the session originates. (U)

STORAGE OBJECT. An object that supports both read and write accesses. (U)

SUBJECT. An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state. (U)

SUBJECT'S SECURITY LEVEL. A subject's security level is equal to the security level of the objects to which it has either read only or both read and write access. A subject's security level must always be dominated by the session security level. (U)

SYSTEM HIGH MODE. See Section V. (U)

TRUSTED SYSTEM. Employing sufficient integrity measures to allow its use for processing intelligence information involving sensitive intelligence sources and methods. (U)

USER. A user is an individual and/or processes operating on his/her/its behalf. (U)

Next 2 Page(s) In Document Denied